

§ 314.1 Purpose and scope.

(a) *Purpose.* This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) *Scope.* This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission (“FTC” or “Commission”) has jurisdiction. This part refers to such entities as “you.” This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§ 314.2 Definitions.

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission’s rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) *Customer information* means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

(c) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§ 314.3 Standards for safeguarding customer information.

(a) *Information security program.* You shall develop, implement, and main-

tain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) *Objectives.* The objectives of section 501(b) of the Act, and of this part, are to:

- (1) Insure the security and confidentiality of customer information;
- (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
- (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

- (1) Employee training and management;
- (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
- (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment,